Kentico

GDPR, Your CMS, and You

GDPR, Your CMS, and You

Published by Kentico Software

GDPR, Your CMS, and You

The Advantages of Putting a GDPR-savvy CMS at the Heart of Your Tech Stack

By

Duncan Hendy, Rich Madigan, Bryan Soltis,
Amy Strada, David Komarek, and Pavel Jirik

Contents

Introduction

Welcome to *GDPR, Your CMS, and You*, a step-by-step guide to familiarizing yourself with all things GDPR, as well as the roles and processes you need to be aware of to help ensure that you comply fully with the regulation and avoid that painful fine. Importantly, this book is written by experts from the worlds of CMS and digital agencies who share their valuable first-hand experience with you. Although this book is intended to guide you through the quagmire of GDPR, we still recommend consulting with your lawyers.

When we first started planning the content and commissioning the writers, we realized that the road to GDPR compliance was not always a straightforward one, especially in terms of responsibility and actionable steps. That's why we have divided our book into two sections: 1) theory and 2) practice.

In the first part, we address who is affected by GDPR, and, specifically, what digital agencies and their clients need to know about data breaches, right to access, data portability, etc.

The second part then focuses on how you achieve this compliance using a GDPR-savvy CMS such as Kentico 11. It shows you the way to handle right to access, data portability, and right to be forgotten, and even track the consents on your website, helping you avoid unpleasant fines. You can see details about our GDPR and Data Protection feature here.

DISCLAIMER

All data and information provided in this book are for informational purposes only. Kentico makes no representations as to the accuracy, completeness, currentness, suitability, or validity of any information contained herein. We recommend consulting with a lawyer for any legal advice pertaining to GDPR compliance.

CHAPTER 1

GDPR and You – An Introduction – Part 1

By Duncan Hendy

Although GDPR is a very real fact, many people have still not grasped the depth and severity of it. But willful ignorance is not something the law will abide, so beware.

In part one of our introduction to GDPR, we look at the new EU regulation from the basics up and try to explain the background to the law, whom it applies to, and some of the things that you are lawfully obliged to implement. With the promise of expensive fines and stringent prosecution, this is something that will have a significant impact on business both inside and outside the EU.

Let's take a look at the background to GDPR and get a deeper picture of how it affects you.

What is GDPR?

GDPR is an acronym for General Data Protection Regulation. It is an EU regulation that has generated the biggest changes in data protection in the EU since 1995. GDPR was created to bring as much uniformity into data protection as possible. That's a big change from the previous situation. There was an existing EU 1995 Directive, which was implemented into national data protection laws. However, there could still be significant differences among states. Now that it is a regulation, it will be directly applicable. It also means that if someone wants to do business in Ireland, for instance, they can now be sure that a similar legal regime will exist in other member states too. This new regulation is better suited to the challenges our current digital world poses.

When Is GDPR Effective from?

GDPR is effective from May 25, 2018, but the final text has were available prior. In all member states, there is a public authority that is responsible for dealing with GDPR issues from an administrative point of view and for imposing any fines arising from non-compliance. Although the regulation is more or less standardized throughout the EU region, there are some areas where member states still have the ability to create amendments to the rules. For instance, there is a rule under GDPR that states children under 16 must obtain the consent of a parent or guardian, but this can be modified to the age of 13. As GDPR states, “the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.”

How Is GDPR Implemented and How Can Companies Prove They Are Compliant?

It is the responsibility of the company to prove that it is compliant under the principle of accountability. This means, they must be able, at anytime, to prove they are GDPR compliant. But as there are several mechanisms that are not ready yet, GDPR wants different sectors to create codes of conduct that say if companies within that sector implement them, those should be enough to prove GDPR compliance. And when these codes of conduct have been approved, companies can implement them and say they are GDPR compliant. GDPR states, “The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.”

Whom Does GDPR Apply to and Who Is Exempt?

According to GDPR, it is an EU regulation that "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." (A controller is the person that determines the purposes and manner in which personal data is processed.) This confirms the establishment is a "broad" and "flexible" phrase not hinged on any legal form. An organization may be established regardless of the size of its operation in the EU.

It also applies to companies outside the region that monitor the behavior of people within the EU, and to non-EU companies that offer goods or services within the EU. So, having a CMS that can distinguish between visitors based within and outside the EU is of great benefit, meaning that, based on geolocation, they do not use analytics on those EU-based visitors without obtaining their consent stating they agree for the site to track their web behavior.

Important to note, one thing that GDPR states is you cannot refuse to provide a user access to your service if they do not consent with processing data collected that is not necessary for the business itself—for instance, if someone visits an e-commerce site to purchase something and the website says that they cannot complete the sales process if they don't let them track their web behavior.

When the only information the page is collecting is the information necessary to complete that purchase, such as name, surname, ID number, etc., it is not necessary to give consent as this is needed for the sales or service contract. But they cannot tell a customer that if they do not give their personal data for their Facebook remarketing, etc., that they are not allowed to buy anything. GDPR states, “when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”

How Much Restructuring Is Involved for Companies?

This depends on the type of data processing the company does, how important personal data use is to their core business, and what type of data it is— sensitive or standard—as there are much higher requirements for sensitive data. That’s why any restructuring based on GDPR should start with a GDPR compliance audit and a deep review that maps the processes with data. The review or audit should then detail what you need to do to implement any procedures or control mechanisms, for example, access rights to certain data.

Who Should Lead GDPR Implementation?

Many bigger companies have started the processes already and have internal compliance officers or external providers of this service. In small-to-medium-sized businesses, this should start with the top management, and they then need to delegate the responsibility.

If You Are a Digital Agency, What Should You Do for Your Clients, and What Is Their Own Responsibility?

Digital agencies, in most cases, are data processors, meaning, they need to take care of existing contracts with their clients because they include all the instructions for the things the agency can and cannot do with the data. So, they need to review these. As data processors, they will also have an obligation to report any breach of GDPR compliance. As GDPR states, this means the agency "processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest…"

For instance, if they learn that the data controller is doing something that is not 100% GDPR compliant, they should inform the data controller about it. And in doing this, they can really be helping their clients in cases such as when they know the client intends to do a certain type of email marketing but they obtained the contacts in a less-than-100% legal way. By informing them that this is against GDPR, they might save the client from incurring a fine. Moreover, they also have to notify the client about any personal data breach. As the GDPR states, “The processor shall notify the controller without undue delay after becoming aware of a personal data breach.”

Finally, the digital agencies will have to implement “appropriate technical and organizational measures” to protect their data and to prevent any type of data breach. These obligations fall on all data processors. As GDPR also states, “Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

CHAPTER 2

GDPR and You – An Introduction – Part 2

By Duncan Hendy

In this second part, we look at what the responsibilities of companies are and how the rights of individuals affect them.

In part one of our introduction to GDPR, we looked at how GDPR will have an effect not only on those businesses that are based in the EU but also those companies from outside the region that have business interests there. In this week's article, we will delve even deeper into content management systems and personal data, as well as some of the new ways in which individuals will have their rights extended. As with the previous chapter, this chapter is organized into questions and answers to help you find your way around this tricky topic even better. So let’s get stuck into some of the nitty-gritty of GDPR.

In terms of content management systems, in what way will GDPR affect how companies do their business?

Firstly, it is important to point out that there are many features in content management systems that work with personal data. You should start with these features, which can include personal data, such as the type of email, newsletter subscriptions, or web analytics. For example, as I wrote last week, with web analytics, you must be aware of whether and what type of consent you need to have. Moreover, you might need to know what the visitor’s nationality is—these factors are important when assessing the applicability of the GDPR for a visitor from a particular country. For email marketing, you need to collect the email address lawfully, for example, you need to get proper consent from the data subject to use their email to send newsletters, etc.

And there are new rights that the data controllers must be capable of providing the data subject with. For example, the right that the data subject can request a copy of all the personal data you collect about them. Your CMS should be able to export the data to give it to the client. And the data subject also has the right to take all of that data you give them somewhere else and upload it into a different CMS. So the content management system must be able to export and also import the data.

Should organizations appoint a Data Protection Officer (DPO)? Is there a workaround?

This depends on the type of the organization. In general, there are three different scenarios in which a company has to appoint a DPO.

- The first one is if the processing is carried out by a public authority or body.

- Secondly, for private companies, the conclusion depends on whether their core activity depends on them collecting and processing personal data, meaning, those are the key operations necessary to achieve the controller's or processor's goals. They have to appoint a DPO if their core activities require the systematic and regular monitoring of data subjects on a large scale.

- The third thing is if, as a core activity, the organization processes special categories of personal data (sensitive data) or personal data relating to criminal convictions and offenses. By special categories of data, GDPR means things such as *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."*

- One thing that might exempt many companies is the large-scale criterion. However, there is an opinion of the special

Article 29 Working Party, which is an EU body interpreting data protection rules. It published examples of large-scale work, such as: "*processing of customer data in the regular course of business by an insurance company or a bank, processing of personal data for behavioural advertising by a search engine or processing of data (content, traffic, location) by telephone or internet service providers.*" They believe a lot of companies that are not undertaking such sizes of work will be exempt from the large-scale criterion.

- Although many companies are exempt based on previous criteria, it can still change based on the Member State's national legislation. For instance, in Germany, where the conditions for DPO appointment are usually stricter.

What rights do individuals have under GDPR?

I have already mentioned data portability rights. Then there is the right to have personal data processed lawfully. There are notification rights, where an individual must be informed that their personal data will be processed and they can ask companies directly whether they are using their personal data. Then there is the most famous right—the right to be forgotten or the right to erasure. It means that data subjects have the right to demand that a data controller erases all personal data they have about them. However, there are situations in which the data controller is not obliged to erase the personal data, such as freedom of expression and information, public interest, etc.

And, of course, the CMS must be able to do this. And it also includes other places where the company has shared the information, for example, CRMs, as well as to other subcontractors or parties.

Everyone talks about GDPR as if it is the devil incarnate. What are the positive aspects of it?

Individuals have a lot of rights and power over which personal data is collected. It should make things as transparent as possible. And if a person consents with personal data being processed, they consent with something they understand and of which they know the consequences. The EU accepts that personal data has value and it’s necessary to protect it and keep it secure. Plus, there is the clarity of responsibility. And companies that state that they are fully GDPR compliant, then the impact could mean the reputation of the company increases. So it is not all doom and gloom.

CHAPTER 3

GDPR and Non-EU Companies – Where Is the Line Drawn?

By Duncan Hendy

Geographical implications and applicability seem to be gray areas for some. Where the borders of applicability lie for those companies based outside the EU can appear confusing. So, let's clear away many of those doubts by addressing some of those key GDPR criteria affecting non-EU-based companies.

In this two-part mini-chapter GDPR series, we will talk about factors that must be taken into account based on geography, not just for the companies themselves, but also the ramifications for their businesses based on the places in which they carry out their business, either knowingly or otherwise.

So let's jump to our first hypothetical scenario: If you are a US-based company but selling to EU companies, obviously, you fall under GDPR. But what about if you are US company but not selling to EU but collecting analytics data on EU located visitors? What are the conditions that cause a company or their actions to fall under GDPR?

It is true that non-EU companies process personal data pursuant to their local data protection regulations. However, there are specific situations in which non-EU companies will have to comply with GDPR requirements. In the following paragraphs, we will go through the rules in GDPR, in particular, Article 3 of GDPR on the territorial scope, and explain these types of situations to you:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

According to case law, the term "establishment" should be interpreted broadly and flexibly. An organization is established if it exercises any real and effective activity—even a minimal one—through stable arrangements in the EU.

For example, if a company has a legal representative in the EU with a contact address or a bank account for the purposes of providing the company's services, the data processing associated with the activities of this entity is subject to the requirements of GDPR.

Another example is sales offices in the EU that promote or sell advertising or marketing targeting EU residents.

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

2. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union

It must be apparent that the organization envisages that activities will be directed to EU data subjects. Examples: intentional use of an EU language/currency, ability to place orders in that language and references to EU users or customers, payment for marketing activities directed at EU users, EU phone numbers, EU top level domain names, etc.

3. the monitoring of data subjects' behaviour as far as their behaviour takes place within the Union

In particular in online business, if you are monitoring the behavior of users that takes place within the EU, you have to comply with the requirements of GDPR. This affects the use of different types of web analytics tools, as well as tracking for personalization purposes. It applies to website visits from users that are in the EU, regardless of whether they are EU citizens or not.

On the other hand, the rule is also often interpreted in the way that the monitoring of EU citizens that are, at the moment of the website visit, located outside of the EU—this is not subject to GDPR.

4. If you have a contract with a client from within the EU or a client applying GDPR

This situation is for an outside-of-the-EU agency/company doing some work for your EU clients that includes personal data (email marketing, web analytics, data storage, etc.). In this situation, you are in the position of a data processor and the client is a data controller. This means your relationship should be governed by the data processing contract under Article 28 of the GDPR and you are allowed to do only what is in the contract and must implement all measures stated there. The data controller must comply with GDPR, therefore, the contract would require you to use such methods/measures that are in accordance with GDPR. Therefore, indirectly, you need to be able to comply with GDPR.

To be more specific, the contract between you and your EU client should stipulate, among other things, that the processor:

- processes the personal data only on documented instructions from the controller
- takes all measures for data security purposes
- taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR
- assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR taking into account the nature of processing and the information available to the processor

Conclusion

In conclusion, every non-EU client will have to evaluate the specific details of their data processing activities in the light of these requirements and decide on the necessary steps to take. It also means that those directly involved in the execution of them must be aware of their responsibilities, and how they fit into the grander scheme of things.

CHAPTER 4

GDPR and Non-EU Companies – A Deeper Dive

By Duncan Hendy

Let's cut to the chase and look in greater detail at more specific aspects of GDPR affecting those companies outside the EU. And more importantly, how they affect you.

In the first part of this mini-guide, I focused on clearing away the doubts that GDPR had created. In this chapter, we answer some questions to add further clarity in specific use cases. These are the more geography-specific topics that can appear confusing, especially when it comes to responsibility and potential incurrence of penalties.

As an evaluation, it is very important to stress again that there are two different positions for a non-EU company where a company would have to comply with GDPR obligations. Either it is based on the activities of the company (in cases 1-3 in the previous chapter) or the company is a sub-contractor of an EU-based company (case 4 in the previous chapter). With this in mind, you can read these additional questions on the topic of GDPR applicability.

The articles of GDPR that are particularly applicable are 28, relating to the carrying out of a Data Processing Agreement, and 46 and 49, regulating personal data transference between EU and non-EU parties.

What steps should organizations undertake in order to determine whether they are bound by GDPR internationally?

It is necessary to be familiar with the four points raised in the previous chapter as they deal specifically with non-EU companies conducting business with or performing analytics on visitors/customers from within the EU. Based on these situations, use common sense to see if they apply to you. It is advisable, in most cases, to consult a lawyer to be really sure.

If non-EU firms are only analyzing visitor behavior, do they need to be GDPR compliant in all areas of their business, even if they are not breaching GDPR in those other areas too?

GDPR is valid for personal data processing in all situations specified in the last chapter. If you do not fall under these conditions that make GDPR applicable, you will still have to comply with your own country’s legislation. Therefore, when analyzing the behavior of a visitor from the EU, the controller is governed by GDPR. However, for other visitors, companies do not need to be GDPR compliant. But, as I have already mentioned, there might be specific rules in the laws of specific non-EU countries, including yours, so be sure to consult your lawyer.

If I have a sub-contractor from outside the EU, what is the legal regime of such a situation?

By sub-contracting to a company from outside the EU, a data controller is granting someone outside the EU access to personal data.

It means that the sub-contractor will process that personal data and, therefore, the data controller must satisfy the legal requirements for personal data transfers to third countries.

It means that in the case of a business relationship between an EU-based controller and a processor outside the EU, the parties have to follow one of the options for data transfer specified in Articles 44-50 of the GDPR.

To answer the question: GDPR is the primary regulation for the legal regime of such a situation. However, in order to use such a third-party service lawfully, there might be additional requirements based on the country outside the EU of the data processor.

Therefore, the final answer depends on the specific circumstances of the case.

What are the different types of options for data transfer?

- For some countries, the European Commission issued an "adequacy" decision, and it is possible to transfer personal data without any further authorization ("safe countries")
- For some countries, a special certification mechanism was implemented, and if the company gets certified, it is possible to transfer personal data in accordance with the certification (in particular with the United States)
- You may transfer personal data, if you implement other appropriate safeguards
- You may transfer personal data under specific situations under Article 49

On the subject of data transference, which countries are considered safe?

Many countries have domestic laws governing personal data protection, and in some cases, these local laws are in fact stricter than GDPR is.

However, the European Commission has shortlisted Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, United States, and Uruguay as being safe countries. This list cannot be considered final because iwt will still be subject to further amendments of GDPR where it could be superseded or, indeed, cancelled altogether. Other countries not on this list are, in particular, bound by Article 46.

What are other appropriate safeguards?

As an appropriate safeguard, you may use one of these mechanisms:

a. a legally binding and enforceable instrument between public authorities or bodies

b. binding corporate rules

c. standard data protection clauses adopted by the Commission

d. standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure

e. an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

f. an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights

What are the derogations under Article 49?

Derogations can be applied under Article 49 under the following conditions:

a. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request

b. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequate decision and appropriate safeguards

c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person

d. the transfer is necessary for important reasons of public interest

e. the transfer is necessary for the establishment, exercise or defence of legal claims

f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

g. the transfer is made from a register that, according to Union or Member State law, is intended to provide information to the public and that is open to consultation either by the public in general or by any person that can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

A data controller could incur a penalty if they fail to ensure GDPR compliance. This means companies acting as a processor for a European data controller are duty-bound to protect their customers through the provision of appropriate data transference.

CHAPTER 5

Who’s Responsible in the Client-Agency Relationship?

By Rich Madigan

From May 25th, 2018, the GDPR (General Data Protection Regulation) is effective. Depending on your viewpoint, this either sees the digital landscape overshadowed by the EU-branded Death Star or represents a brave new world. Either way, the landscape as we know it radically changes the way organizations handle and store personal data.

There are hundreds of articles, posts, and opinion pieces swirling around the web, from scaremongering through to helpful bite-sized guides. Sifting through all of this information, you can piece together the sheer scope of work involved in achieving GDPR compliance both internally (with regards to your employees and prospective employees) and externally (with your customers and prospective customers).

With the GDPR coming into force, the likelihood is that you have a mountain of tasks to undertake. The new regulation touches many aspects of your business and, while the digital agency only interfaces with a small part of that, it still has a key part to play.

In this part, I'm going to explore the three key roles within the GDPR—the Data Controller, the Data Protection Officer, and the Data Processor.

The Data Controller

In a nutshell, the Data Controller states how and why data is processed.

Within my universe at MMT, the view is clear. Data Controllers are our clients, and this is typically the case across the board for companies. If you're capturing user data for sales or marketing purposes, the chances are that you are the Data Controller.

The Data Controller is typically an organization, but there are cases where an individual is the Data Controller, e.g., self-employed, freelance consultants, and contractors.

Under the old law, the buck stopped with the Data Controller. This put the burden of responsibility solely on the Data Controller. The GDPR mixes this up, and responsibilities are now shared between Data Controllers and Data Processors. However, it is fair to say that the Data Controller is still the key figure. They are responsible for ensuring compliance across the business, communications with supervising authorities, handling user requests (right to be forgotten, right to portability, etc.) and working with their Data Processors to establish reasonable processes to support compliance.

The Data Protection Officer

The Data Protection Officer is a mandatory role that has been introduced as part of the GDPR. The Data Protection Officer is a company's expert on the GDPR and is responsible for educating on compliance, monitoring compliance, and being the point of contact for the supervising authority (e.g., the Information Commissioner's Office). You can find more information on the ins and outs of the role here.

For many of the Data Controllers out there, a Data Protection Officer is a required role. There are specific guidelines in place for when you must appoint a data protection officer, which you can find on the ICO website.

The role and responsibilities of the Data Protection Officer are not to be underestimated. Based on the sheer scope of the GDPR, whoever is appointed to this role will have their hands full and should be dedicated to this role.

If you have not appointed a Data Protection Officer, then you must have staff within the business that fully understand the GDPR and your obligations—to the same standard as would be expected from a Data Protection Officer.

As you scour through the droves of articles, you will see many parties calling for a Data Protection Officer to be appointed within each Data Processor (for each client of the Data Processor), and this is actually referenced in the articles of the GDPR.

The Data Processor is likely to have their own DPO for their own compliance as a business but, when it comes to clients, this should be treated case-by-case to understand exactly what level of contact he/she has with the user data.

The Data Processor

The Data Processor processes the data on behalf of the Data Controller.

So, if we take MMT Digital, we would be the Data Processor for our clients. However, this responsibility could also lie with our client's hosting provider or any SaaS vendors they use (e.g., Salesforce). However, the caveat here is that this only applies when the party in question has access to the user data.

The first step is to work out if your digital agency is a Data Processor. You need to understand what contact they have with your user data (if any). You'll need to do it as part of your own data mapping exercises, so why not kill two birds with one stone?

If they don’t have access, it isn’t necessarily the end of the road. While your digital agency may not shoulder the responsibilities of the Data Processor, you can still call upon their expertise to understand how and where data is stored to help you in your own data mapping plans.

However, if you have established that your agency is a Data Processor, you need to:

- work with your agency to put together contracts or SLAs to define how they can interact with the data (Data Processing Agreements).
- establish whether there are “sub”-Data Processors involved, understand what they have access to, why they have access, and then remove that access or get agreements in place.
- establish written instructions and guidelines on how personal data can be processed by the Data Processor.
- put in place an audit framework to contain records of data processing activities. The Data Processor should have input as they will understand the technology but the Data Protection Officer can take the lead as they understand the exact requirements.
- set up communication channels for supervising authorities.
- establish processes for breaches, right to be forgotten, etc. (more on this in a later blog post in our series!)
- establish whether a Data Protection Officer is required in the Data Processor.
- understand the requirements around cross-border transfers.

CHAPTER 6

GDPR – Who's Responsible for Data Security and Breach Notifications in the Client-Agency Relationship?

By Rich Madigan

Welcome to the next chapter exploring the practicalities of the GDPR in the client-agency relationship. In this part, we'll be delving into data breaches. Data security is a key theme within the GDPR and there are much stricter obligations on Data Processors and Controllers alongside guidance.

We can split this into two parts—data security and breach notifications.

Data Security

First up is data security. As we've touched on in previous chapters, there's a shared responsibility from the Data Controllers and the Data Processors to ensure that data is stored, processed, and handled securely. For Data Controllers, it is important to only engage with Data Processors that can demonstrate not only compliance with the GDPR, but also "security of processing" standards.

There's a range of security actions to consider, including pseudonymization of user data, security around processing systems and services, restoration of data following any incidents, and evaluation processes.

As we have already stated, processes and standards that are agreed between the client and the agency are key here. While they make up a small part of the overall working relationship between the client and the agency, they are crucial in achieving compliance.

Agreeing these standards does not need to be an overly complex process. The Data Processor/agency will have standards surrounding data security—drawn from coding standards, encryption standards, and OWASP.

Working in collaboration with the agency, the Data Protection Officer (and the Data Controller in general) can work to understand the standards in place and use these as the foundation for setting project-specific and account-specific processes and standards to enable current and future digital projects to achieve compliance.

Breach Notifications

Next up is the tricky world of breach notifications. With the murky waters of responsibility in the past, it was difficult to know who should be notifying whom. The GDPR has clarified this considerably and it is easier to understand exactly what a breach is, and who needs to do what.

Let's start with the notion of a "personal data breach". Under the GDPR, this is classified as a breach of security that causes the accidental or unlawful destruction, loss, modification, unauthorized access, or unauthorized disclosure of personal data that is being held, transmitted, or processed.

The notifications we need in place all hook into this definition of a "personal data breach". There's some clear directions on what the Data Controller should do and what the Data Processor should do.

For the Data Controller, they have two sets of notifications.

The most common relates to the supervising authority. They must notify the supervisory authority (e.g., ICO in the case of the UK) within 72 hours of becoming aware of the breach. If notification isn't made within 72 hours, there has to be a very good reason. These notifications need to outline the nature of the breach clearly, provide contact details of the relevant people at the Data Controller (including the Data Protection Officer), describe the likely consequences of the breach, and explain how you are going to resolve the breach.

The second relates to your customers. This only applies when the breach in question is likely to introduce a high risk to the "rights and freedoms" of your customers. You need to communicate the nature of the breach and how you are going to resolve it as soon as possible.

There's an exemption around this where notice is not required if the breach is unlikely to risk the rights and freedoms of your customers. It's a big field of debate and creates a bit of grey area. The safest bet is to stick to your notifications.

For the Data Processor, their responsibility is to notify the Data Controller as soon as they become aware of the breach but they have no other notification or reporting obligation under the GDPR.

That covers the requirements of the GDPR, but the question is how it should work in practice. Like with most things GDPR-related, the key is communication and collaboration. The Data Controller and Data Processor need to work together to put in place the processes and tools that will make those notifications as easy as they can be. This is going to include mainly, but not exclusively:

- identifying the appropriate monitoring tools
- identifying processes for routine breach checks
- establishing a documented procedure for the agency (Data Processor) to report breaches—complete with audit trail!

- agreeing upon SLAs to cover notifications between the agency (Data Processor) and the client (Data Controller)

This is obviously the tip of the iceberg, and there's all sorts of other processes that the Data Controller is going to need in place. But, hopefully, this gives you a starting point in at least ensuring alignment between yourself and your agency.

CHAPTER 7

GDPR – the Right to Portability

By Rich Madigan

In this next part, we continue exploring the practicalities of GDPR in the client-agency relationship. This time around I'll be exploring the "right to portability", specifically what it is and what impact it has on implementation and operations within a project. It is another important part of GDPR that should be aware of.

What Is It?

So, continuing from my previous chapter, one of the aspects of GDPR is that customers are now in control of their data. If they so wish, they could take all of the data you hold on them and sell this on to another Data Controller (e.g., a research company). Once the customer requests the data you have on them, it is your job as the Data Controller to then provide all that information in a “machine readable” format (e.g., XML, JSON, CSV) within a reasonable timeframe.

However, there are caveats to this that you should be aware of. The data covered by this right only includes:

- Data provided by the customer to you (e.g., through a form)
- Data that has been processed by automated means (e.g., data captured by online marketing software, data from a fitness tracker, location data)
- Data that has been processed based on explicit consent or the fulfilment of a contract

Data outside of this is not considered within the scope and there is no obligation to deliver this data to the customer.

In addition, data portability is not an absolute right. The Data Controller needs to assess the legitimacy of the request, e.g., it will need to be weighed against the rights of others.

What Do You Need to Consider?

Data portability potentially has a large impact on your business. It can be split into three specific challenges:

- Technical – being able to extract the data efficiently largely depends on the capabilities of the systems in place. Any inefficiencies could incur large costs for the business.
- User Experience – the process needs to be as simple as possible for your customers.
- Business strategy – this right allows for the possibility that customers can move their data between you and your competitors so you need to consider this in your strategy from the outset.

Of the three challenges, the agency (Data Processor) can have an impact on the first two options but not explicitly the third.

Your “right to portability” process should consist of the following items:

- the mechanism(s) that the customer can interact with to initiate the process
- the mechanism(s) for exporting the customer’s data
- the process to be followed and the accompanying audit trail
- the reporting mechanism to the customer (e.g., email notification of the process being initiated)

How Can Your Agency Help?

As I’ve intimated in previous chapters, the scope of customer data available to the agency (Data Processor) is a few pieces of the jigsaw. There’s a larger challenge facing you (the Data Controller) and you will be ultimately responsible for getting the systems and processes in place, but your agency (Data Processor) has a part to play in fleshing these out.

This can be broken down into a set of steps for you and your agency to work through to plan and implement the required processes and functionality.

- The process starts with identifying the systems and channels that your agency is working on for you, e.g., website, marketing software. We need to be clear on what should be covered in the process.
- You then need to understand what functionality is provided by the CMS or solution underpinning the project, in particular the functionality related to the data portability.
- You then need to identify the gaps. The DPO can provide support here to lay out the entire functionality required to achieve compliance and you can then identify missing functionality and map out the work involved in fleshing out these gaps. This is going to include ensuring that there is a sufficient audit framework/trail in place.
- You also need to consider the underlying process and how this functionality will tie into the process. This will include defining timescales.
- With all of this in place, you can then implement the required functionality.

The entire process should be documented for auditors/investigators and may need to be factored into SLAs and contracts established between you and your digital agency.

What’s Next?

Hopefully, these chapters have given you an insight into the types of conversations that should be happening between you and your agency. GDPR is a massive topic with implications reaching throughout your organization.

CHAPTER 8

I’m a Developer and General Data Protection Regulation (GDPR) Is No Big Deal. Or Is It?

By Bryan Soltis

I’ve been a developer for nearly 20 years. Over that time, I have weathered my share of regulations and standards. I’ve seen PCI and HIPAA rush in like a gang of silverback gorillas and upheave a development team in a single blow. Y2K? Forget about it! I sat and prayed that planes didn't fall out of the sky while updating SQL 6.5 databases to four-digit years. When I first learned of GDPR, naturally I wasn't quivering in my boots too much. Maybe I should have been. And maybe you should, too.

General Data Protection Regulation (GDPR for the cool kids in the know). Not a very exciting sounding name, is it? If it was really serious, it would be something like "Tactical Obliteration of Information Initiative"(TOII—trademark pending), right? Style points aside, this little acronym is causing quite a stir in organizations around the world. From banking to education, companies are beginning to place their bets on just how much of an impact Europe's new regulations are going to have on consumers, businesses, and what is surely to be some record-setting legal fees.

And if you thought it didn't apply to your non-EU site, guess again! GDPR has a global reach, thanks to the whole "everything-connected-via-the-Internet" thing. If you store any information about European users, GDPR will apply to you. Data requests will need to be fulfilled in 30 days. And data breaches? Oh, man! You will have 3 days to get those reported. With 20M Euro fees on the line, everyone should be preparing themselves for the fun.

So, What Is GDPR Exactly?

If you haven't had the joy of sitting through a presentation on the legal impact and ramifications of GDPR, then good for you!

For those of you that have, bear with me as I summarize the new regulations for the other readers.

GDPR is all about protecting people's information in the digital space. As our lives have become more influenced by the information someone has about us, the need for stricter control and oversight is key. With the right information, you can take over a person's complete identity and wreak havoc on their career, relationships, and their eBay Seller profile.

Most of the laws currently in place for online data were drafted back in the mid-1990s. Sure, we had Windows 95, America Online (AOL), and some rocking 56K modem speeds! What we didn't have is a clue about what the next 20 years would bring when it came to what (and how much) information people would be sharing. Over the past two decades, people have chronicled their entire lives on social media and other sites, setting the stage for some serious vulnerabilities.

GDPR is all about trying to control that data and making sure people know exactly how much information a site is storing about them. It's about giving them control over their details and ensuring companies comply with "Right to be Forgotten ", "Underage Consents", and "Data Portability" requests. It's about vulnerability for site owners, and regulating how they handle their users' information.

Uhm, So That Sounds Like a Big Deal

OK, maybe you're like me and have started to sway from your throw-caution-to-the-wind and cook-bacon-without-a-shirt remarks. GDPR is no small thing and comes with a lot of implications for anyone in any industry (yes, especially developers!). The effects run very deep and will certainly not be contained only to EU audiences. Developers need to start educating themselves now to be prepared.

So, what do you need to know about? Of course, there are the basic of the new regulations that every developer should get familiar with. You should fully understand what data GDPR applies to, and what new functionality you need to provide consumers.

When it comes to the technical aspects, there are a few keys areas you will want to know.

Data Flow

GDPR is all about data. This means understanding and reporting what data is being collected, where it's being collected, what happens to the data, and who has access. How people's personal info travels through your organization, is called **data flow**. With the regulations, companies will be required to provide a detailed history of every step a piece of information makes within the organization. This means developers will need to track their client's data, who has access to it, and how the data is used to meet the new standards.

Explicit Consent

For far too long, companies have been able to analyze and leverage people's information for targeted marketing communication, user profiling, or even nefarious reasons, with little to no oversight. GDPR changes all that with requiring companies to get **Explicit Consent** for their users when collecting and using their data. Business will have to present a clear definition of how much of a user's information will be collected, and how it will be used. This regulation is aimed at stopping people's data being used without their knowledge or consent. Developers will need to understand how data is being collected and how it will be used. This means developing a mechanism for obtaining that consent for any user of an application.

Right to Access

People are often willing to give their information to a trusted source. If the organization is reputable, and their intentions are true, most companies won't have a problem with getting consent for data collection. But what happens when a third party of an unknown source gets access to that data? People lose their minds!

GDPR is about giving that power back to the consumer and making sure they know every individual that can access their information, and why. This means developers need to start thinking of how to limit access to user's information, unless there are essential to the business.

Another big part of the GDPR regulations is the requirement to provide individuals with information when requested. Under the new laws, companies will be required to provide a detailed list of all information they have collected and/or storing about a person. And I mean EVERYTHING! Developers should plan now for how they are going to report this information, as the laws require you to provide it within 30 days of the request!

Right to Be Forgotten

Oh, boy, this is a big one! Identifying and reporting on all the data you have about a person is one thing, but giving the user the ability to remove that data is a big deal. One of the most important pieces of GDPR is providing the people with the option to remove all the information a company is storing about them. This means deleting personal information, as well as other identifiable data, all within the required 30-day window once a request is made. For developers, this means you will need to handle this data removal within your application, supplementing dummy data where needed. This can be a big deal, especially if much of your application's functionality is built around personalized, custom information for each user. Just think of a social media site with no personal details about someone!

One thing to note about this data removal is it's not EVERYTHING. For some sites, like e-commerce applications, retaining personal data may be required for reporting and auditing. This means that some sites may need to scrub their data when a user makes a request, however, critical information may be retained to comply with financial regulations and laws. This is where understanding the GDPR laws becomes especially important! Developers need to know when it's appropriate to remove data from their systems, and when it will be required to retain them. That means lots of fun talks with lawyers to hash out each bit of data in your sites!

What Do You Need to Do?

OK, at this point you may be looking up “How to be a potato farmer” or other career changes. Don’t worry, it’s not that bad! You should have a solid idea of how GDPR will impact your applications. You should also know where in your application to update code and add new features. With that information, you can start to take action.

Develop a plan

You know what needs to happen. Now you need to make it happen! You should start by mapping out all the data you found in the discovery phase and break it into logical sections. Understand what areas of the application need to change to accommodate the modifications and start dividing them among your team. You need to recognize resources you may be lacking and work to secure those long before you start your changes. Defining a complete and thorough implementation plan not only looks great on a Kanban board, it also helps you stay on track and understand how long each piece will take.

Remove anything you don’t have to keep

You can save yourself a lot of future headache if you can reduce the amount of data you’re dealing with. Maybe during your research, you found out that your marketing team is storing complete family trees for every user of the site. If this data isn't essential, get rid of it! Review every bit of information you're storing, and see what you can live without. The less sensitive data about your users, the smoother sailing over to GDPR land you'll have.

Limit access, if you can

GDPR has a lot of rules around the data, however, a big part is how that data is stored, backed up, and accessed. Part of your plan should include a long, hard look as to who within your organization has access to the information. You should conduct interviews with personnel, dust off your Disaster Recovery (DR) checklists, and start to limit access to the data where you can. If you find someone that isn't essential, remove them from the list! You'll thank yourself later when it comes to reporting information if you ever get audited.

Get ready to answer a lot of questions

Speaking of reporting information, new regulations are pointless if no one is enforcing them. Because of the impact GDPR is going to have around the globe, there will surely be an audit in your future at some point. Don't sweat it! You should be well prepared to answer any questions you get, and have detailed logs and exciting reports to serve up to your legal team. The more you know about your system and the data, the easier this process will be, so start planning for it now.

Conclusion

As a developer, it's great to be confident. Grit and determination allow you to overcome obstacles and challenges, refusing to admit defeat. When it comes to GDPR, your mettle may be tested. Have no fear, my friend. GDPR is the next evolution in a long line of standards that affect our development life. With proper education and preparation, any developer can handle GDPR with ease. Make sure you are storing data properly and always coding to standards, and you'll be back to coding Easter Eggs in no time!

CHAPTER 9

It’s Time to Go with the (Data) Flow

By Amy Strada and David Komarek

The amount of personal data dissemination that goes on today is astounding. When I sign up for Spotify and I want to use my Facebook login for ease, Spotify receives my contact info, who my friends are, my location, and probably loads of other stuff. And Facebook receives my music tastes, which to some (ahem, me) is basically their soul.

According to GDPR, this rampant data spread has gone on unchecked long enough! Like a neighborhood vigilante, GDPR mandates that companies know exactly where they get data from, to whom they send it, and what they do with it internally. Say hello to data flow mapping! It's like playing Six Degrees of Separation, but with people's birthdays and embarrassing middle school photos.

What's This Thing, Then?

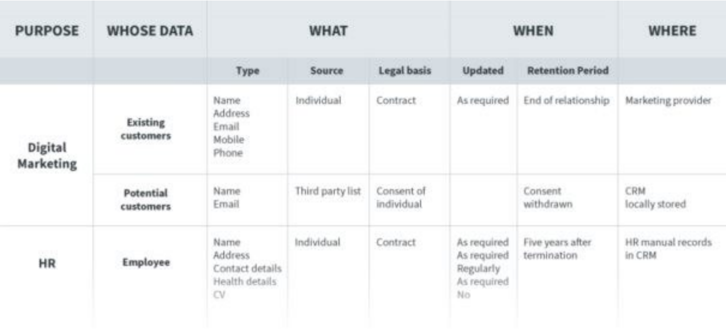
Perhaps obviously (although nothing is very "obvious" about GDPR), data flows are the ways data is given to, sent from, and used within your organization—you know, how data "flows" around you. Ask yourself:

- How is the personal data we receive collected?
- Who is accountable for this data?
- What is the physical location of the data?
- Who can access this info, and is this data disclosed to anyone else?

There are plenty more things you should be aware of, but, you know, I'm not a lawyer. A lawyer (specifically one specializing in GDPR) is good to have around when you're hashing this out. In essence, you need to know as much as you can—within reason—about the data your organization is accumulating.

And How on Earth Am I Supposed to Do That?

Well, there's data mapping for that. This is a good first step to take when doing a GDPR audit as it provides a comprehensive overview of all your data flows. It also allow you to visualize more clearly the directional flow of information surrounding your business. The final product might look something like this:



PURPOSE	WHOSE DATA	WHAT			WHEN		WHERE
		Type	Source	Legal basis	Updated	Retention Period	
Digital Marketing	Existing customers	Name Address Email Mobile Phone	Individual	Contract	As required	End of relationship	Marketing provider
	Potential customers	Name Email	Third party list	Consent of individual		Consent withdrawn	CRM locally stored
HR	Employee	Name Address Contact details Health details CV	Individual	Contract	As required As required Regularly As required No	Five years after termination	HR manual records in CRM

Once you have this in place, you can clearly visualize the ways data is being used. As GDPR's goal in life is to protect people from organizations that might be inappropriately using personal data, this map is immensely integral to preparing yourself for GDPR compliance. If your organization doesn't know where it's getting emails and locations of your users from, how can you know if you are getting this data in a legal and compliant way?

What Is Kentico Doing with Data Flow Mapping?

Quite a bit! We realized we needed to figure out where to start for ourselves before we launched into fixing things for Kentico 11. To prepare, we went through a data flow audit with our own GDPR lawyers, running through our fictional coffee company Dancing Goat's website.

After that, we discussed Kentico's departments and figured out the type of data we were (and are) collecting, most of which comes through forms, some through analytics. We then attempted to answer the questions mentioned above—who is responsible for the data, where we keep it, etc.—as well as figure out whether or not we have any license to process it, be it via a contract, legitimate user interest, expressed consent, or some other vehicle for compliance. And when creating our own data flow map, our documentation for Kentico 11 came in really handy. It was able to save both our and our lawyers' time (and, of course, we saved money).

And even though our audit is not completed yet, it has still eaten up a lot of our time and resources. Mapping everything from scratch will take ages, so it's great to be able to have resources that help you figure out where to start. (Here's hoping more resources like this from vendors begin popping up soon!)

This Is Super Complicated

Can't argue with you there. That's why our developers are working crazy hard to make sure Kentico 11 will help make this a lot less complicated for our users so the job is easier on your end. For example, we can stop the spread of submitted data (let's say an email address) across your entire website if a visitor only wants to download a brochure from you. That data won't be used anywhere else on your website.

As a CMS vendor, we want to make sure our clients are getting the most help we can deliver to prepare for GDPR. We're preparing our Documentation to be ready to help you out with whatever you need. It'll be able to provide you with the basics of how to use our features to get the data you need, and it will certainly save you time and money.

But as I said, neither I nor our developers are GDPR lawyers, and it would make your life infinitely less crazed to consult one when it comes to data flow mapping (and anything GDPR related, for that matter). Digital agencies will need to help their end-clients, and both end-clients and digital agencies need to be GDPR compliant in this area.

You're Sure I Need to Do This?

Sorry, but yes. Article 30 of GDPR states that records of data processing activities must be made and kept. But really, look on the bright side—having these records helps *you* a great deal, as well. Now you know every detail about your users' data. Does something seem nonsensical or maybe even unnecessary? With your data flow map, you can more easily streamline these processes or change them or even delete them altogether.

Let's say you find out that one of your online forms asks for 10 different attributes of your visitors for the purpose of…well, nothing. Maybe you just use the email address to send them a newsletter, but you have no personalization or segmentation in place. Well, in that case, you might consider using the "data minimization" principle and collect only necessary data. In the end, you may find out that you get better conversion rates on your form, and you will also simplify data flow (and also may not require extra consents from your visitors).

You'll also get a clearer understanding of how personal data is used across your company. It seems daunting, surely. But you do benefit at the end of the day.

CHAPTER 10

Tracking GDPR Consents in Kentico 11

By Pavel Jirik

Friday, 25th May 2018… What a date! Friday night full of Champagne drinkers, getting tipsy because they just managed to become GDPR compliant and free from the potential €20M fine!

Digital happiness starts with a GDPR-valid consent from website visitors. But what can you do to achieve this?

There are many things you need to do, but especially if you collect the data of EU citizens and use it to personalize their website experience in some way. In most cases, it is much easier to say than to do, and that's the exact reason why we added the consent tracking functionality to Kentico 11.

As we are always pushing Kentico to newer heights, providing you with the help you need to comply with GDPR was one of our top priorities on the list. Going through the GDPR compliance processes ourselves, we realized how complex the whole thing was, and decided to make it as easy for you as possible.

That's why we added the Data Protection application to Kentico 11 where (among other things) the consents can be created, updated, and stored, to be then displayed on your website wherever and whenever needed.

Of course, there are plenty of other things you need to ensure to become GDPR compliant (and you should discuss it with your lawyers in the first place), but we believe that our improvements will be a great help on your way to GDPR compliancy.

If an image is worth a thousand words, then a video is definitely worth of thousand images. So, let's watch the following video which describes how the tracking consent functionality can be used in Kentico 11:

https://youtu.be/sqX6mE6HWek

Let's recap the two main macros used in the video:

{% !OnlineMarketingContext.CurrentContact.AgreedWithConsent([code name of the consent]) %} -> checks if the current contact hasn't agreed to a specific consent yet (notice the exclamation mark at the beginning of the macro).

{% GlobalObjects.Consents.[code name of the consent]. GetConsentText().FullText %} -> displays a full text version of the specified consent.

These two macros are the most important ones needed for the successful implementation of the tracking consent functionality in Kentico 11.

And let's not forget the short version of the tracking consent that is managed and displayed by the **Cookie Law and Tracking Consent** web part that needs to be placed (ideally) on a master page. It can be configured to display different text per each cookie level, especially the one when a visitor hasn't agreed to a consent yet.

CHAPTER 11

GDPR’s Right to Access in Kentico 11

By Pavel Jirik

If any of your website visitors (or customers) asked you to provide them with all the data you had collected about them so far, what would be your first thought? Would it feel like an easy thing to do, or rather something quite complex, as you would need to gather all the sources and make sure you didn’t miss anything out?

It is no more a secret that with GDPR around, our digital lives within the EU receive a privacy boost. And by boost, I mean a massive one!

Up until now, there hasn't been such a strict EU-wide law forcing businesses within (and even outside of) the EU to take so much care when dealing with our data as the GDPR demands. Yes, there have been companies acting responsibly and fairly, but there have also been many that simply do not care at all.

Furthermore, the new legislation brings some serious overheads, and if not prepared well, it could take you by surprise, literally hitting you like a tsunami! Unless, of course, you are willing to lose up to 4% of your annual worldwide turnover or €20M…

Plus, time is also not on your side, as you need to be fast and answer every request within 30 days or risk facing that financially painful penalty.

Let's Surf the Wave!

But it doesn't have to be so bad. Even though some extra work will always be necessary and unavoidable, there are ways to make the whole GDPR compliance process easier, and allow you faster responses to those "curious" visitors willing to find out what you know about them so far.

Fortunately for you, we have a surfboard to help you ride that GDPR wave! As everybody knows, surfing waves is way more fun than just paddling in them!

Thanks to the previous chapter explaining GDPR consents in Kentico 11, you already know about our new Data Protection application we created in Kentico 11 to help you streamline GDPR processes.

The Data Protection application can be a great help in many GDPR scenarios, but let's focus on the GDPR's right to access.

As soon as you have an email address of the person requesting data access, you can go to the Data Protection application and retrieve all data that has been gathered by the Kentico system. If properly implemented, it can include data from third-party systems and integrations as well. Then it is up to you and your company's internal guidelines what to do further with such data.

Let's watch this video to get a better idea of how it works in Kentico 11:

https://youtu.be/Z8NB2w2lPkc

CHAPTER 12

GDPR’s Right to be Forgotten and Data Portability in Kentico 11

By Pavel Jirik

It’s never easy to let go. But if someone asks you to forget about them, you just need to move on and get over it. That’s exactly the case of GDPR’s right to be forgotten. If any of your website visitors ask you to delete all their personal data, you have to do it. To make it slightly more difficult, there are some situations where you actually need to keep some of the data due to legal reasons.

In some other cases, the one who requested data deletion may have asked you to delete just some of the data. For example, their website activities or submitted forms.

As you can see, there is a lot of what can be requested, and we tried our best to deal with it in Kentico 11. It will never be bulletproof, as every company, business, or website has their own policies, rules, and integrations. But with the Data Protection application, much of the effort can be streamlined.

Bring It On!

If someone requests their data's deletion based on the GDPR's right to be forgotten, your first steps in Kentico 11 should lead you to the Data Application app and its Right to be forgotten tab.

Based on their email address, you can search for all the known data of the person and decide what should stay in the system and what should be deleted by selecting the relevant checkboxes after clicking the "Select data to delete" button.

Think twice before you delete the data, though! As it will be deleted from the system for good, and unless you have a latest backup of your database, it will not be recoverable.

There are quite a few checkboxes that can be ticked. If all of them are left selected, then Kentico deletes all the data related to the contact (visitor). But as we wanted to give you much greater flexibility, you can delete only very specific data, as necessary. For example, if you want to delete only the newsletter subscription related data of the contact, you can! Do you wish to delete only the customer related data? No problem! Would you rather delete just the submitted forms' data? Well, you are the boss! Deleting just the activities of the contact? Consider it done!

How does that sound? Not hard at all, is it? You can be sure that the GDPR will throw some punches at you, definitely! Sometimes they will be easy, and sometimes they will be tougher, but with the right software solution, lawyers, and developers, you should be able to deal with the GDPR's requests well.

True, you will need to stay super conscious in the upcoming years and decades, but in the end—it's the safety of our (and your) personal data! No one likes to share their personal data with strangers…

Data Portability

There is also another thing that the Data Protection application can help you with. For whatever reason, any digital soul can ask you to send them all their data. But this time, they may want it in a machine readable form.

It could be because they want to look more cyborg, but on a serious note, they may just have decided to copy the data from one system into another. They may also need it for their own purposes, to just have a personal backup of the data.

Whatever the reason, in such a case, IT environments need to understand each other, and the best way to achieve it is by using a standardized approach. One of many, could be XML output, and that's exactly what Kentico 11 does.

This way, the data can be easily transferred from the Kentico system into another one, and no bits are lost.

The difference between a simple list generated on the Right to access tab (if you haven't read the chapter on this topic yet, feel free to dive into it), and the XML output on the Data portability tab is that the XML output contains even some other system related data. For example, the value of the ContactGUID property of the contact. It is a unique value that identifies the contact in the Kentico database (the marketer cries, the developer smiles).

Whether you need to deal with a data transfer or data access request, it should be simple for you now to distinguish between them both.

Once again, both “Data portability” and “Right to access” tabs are almost identical. Only the output is different.

It is entirely up to you how you leverage the listed data, but it always needs to follow the internal GDPR processes defined within your company.

The GDPR storm can be withstood just fine, as long as you give yourself enough edge through the right tools and know-how!

Afterword

Thank you for taking the time to read our book *GDPR, Your CMS, and You*. We are sure that it has clarified a lot of the issues that have arisen due to GDPR. We learned from our own experiences with performing an internal data audit that being compliant with GDPR was not as straightforward as some people might expect. And using this experience, we created Kentico 11's Data Protection feature to make GDPR compliance even easier, especially in the areas of data portability, right to be forgotten, right to access, consents management, and data flow mapping. Check out the feature for yourself here.

DISCLAIMER

All data and information provided in this book are for informational purposes only. Kentico makes no representations as to the accuracy, completeness, currentness, suitability, or validity of any information contained herein. We recommend consulting with a lawyer for any legal advice pertaining to GDPR compliance.

Kentico

www.kentico.com